CLAIMS

1. An information recorder for recording information to a recording medium, the apparatus comprising:

a transport stream processing means for appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; and

a cryptography means for generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated;

the data encrypted by the cryptography means being recorded to the recording medium.

2. The apparatus according to claim 1, wherein the cryptography means generates the block key for encrypting the block data from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

3. The apparatus according to claim 1, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key

unique to data to be recorded to the recording medium, and generates the block key from the title-unique key and block seed.

4. The apparatus according to claim 1, wherein the cryptography means generates a disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and stores them into the recording medium.

5. The apparatus according to claim 1, wherein the block seed includes copy control information in addition to the arrival time stamp (ATS).

6. The apparatus according to claim 1, wherein the cryptography means encrypts, with the block key in the encryption of the block data, only data included in the block data and excluding data in a leading area including a block seed of the block data.

7. The apparatus according to claim 1, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, takes the thus-generated title-unique key as a key for an encryption function, places the block seed into the encryption function, and outputs a result of the placement as a block key.

8. The apparatus according to claim 1, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key

unique to data to be recorded to the recording medium, places the title-unique key thus generated and block seed into a one-way function, and outputs a result of the placement as a block key.

9. The apparatus according to claim 1, wherein the cryptography means generates a device-unique key from any of an LSI key stored in an LSI included in the cryptography means, device key stored in the information recorder, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and generates a block key for encrypting the block data from the device-unique key thus generated and block seed.

10. The apparatus according to claim 1, wherein the cryptography means encrypts block data with the block key according to a DES algorithm.

11. The apparatus according to claim 1, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not recording to the recording medium is allowed.

12. The apparatus according to claim 1, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is allowed.

13. An information player for playing back information from a recording

medium, the apparatus comprising:

a cryptography means for decrypting encrypted data recorded in the recording medium by generating a block key for decrypting encrypted data of a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and

a transport stream processing means for controlling data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted by the cryptography means.

14. The apparatus according to claim 13, wherein the cryptography means generates the block key for decrypting the block data from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

15. The apparatus according to claim 13, wherein the cryptography means generates a title-unique key from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and generates the block key from the title-unique key and block seed.

16. The apparatus according to claim 13, wherein the block seed includes copy

control information in addition to the arrival time stamp (ATS).

17. The apparatus according to claim 13, wherein the cryptography means decrypts, with the block key, only data included in the block data and excluding data in a leading area including a block seed of the block data.

18. The apparatus according to claim 13, wherein the cryptography means generates a title-unique key from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, takes the thus-generated title-unique key as a key for an encryption function, places the block seed into the encryption function, and outputs a result of the placement as a block key.

19. The apparatus according to claim 13, wherein the cryptography means generates a title-unique key from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, places the title-unique key thus generated and block seed into a one-way function, and outputs a result of the placement as a block key.

20. The apparatus according to claim 13, wherein the cryptography means generates a device-unique key from any of an LSI key stored in an LSI included in the cryptography means, device key stored in the information player, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and generates a block key for decrypting the

block data from the device-unique key thus generated and block seed.

21. The apparatus according to claim 13, wherein the cryptography means decrypts block data with the block key according to a DES algorithm.

22. The apparatus according to claim 13, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not playback from the recording medium is allowed.

23. The apparatus according to claim 13, further comprising an interface means for receiving information to be played back from a recording medium, and identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not playback the recording medium is allowed.

24. A method for recording information to a recording medium, the method comprising the steps of:

appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; and

generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated;

the data encrypted in the cryptographic step being recorded to the recording

medium.

25. The method according to claim 24, wherein in the cryptographic step, the block key for encrypting the block data is generated from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

26. The method according to claim 24, wherein in the cryptographic step, a title-unique key is generated from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and the block key is generated from the title-unique key and block seed.

27. The method according to claim 24, further comprising the step of generating a disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and storing them into the recording medium.

28. The method according to claim 24, wherein in the cryptographic step, only data included in the block data and excluding data in a leading area including a block seed of the block data is encrypted with the block key in the encryption of the block data.

29. The method according to claim 24, wherein in the cryptographic step, a title-unique key is generated from a master key stored in the information recorder, disc

ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated is taken as a key for an encryption function, the block seed is placed into the encryption function, and a result of the placement is outputted as a block key.

30. The method according to claim 24, wherein in the cryptographic step, a title-unique key is generated from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated and block seed are placed into a one-way function, and a result of the placement is outputted as a block key.

31. The method according to claim 24, wherein in the cryptographic step, a device-unique key is generated from any of an LSI key stored in an LSI included in the cryptography means, device key stored in an information recorder, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and a block key for encrypting the block data is generated from the device-unique key thus generated and the block seed.

32. The method according to claim 24, wherein in the cryptographic step, the encryption of block data with the block key is made according to a DES algorithm.

33. The method according to claim 24, further comprising the step of identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not

recording to the recording medium is allowed.

34. The method according to claim 24, further comprising the step of identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is allowed.

35. A method for playing back information from a recording medium, the method comprising the steps of:

generating a block key for decrypting encrypted data in a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and

processing a transport stream processing means to control data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted in the decrypting step.

36. The method according to claim 35, wherein in the decrypting step, the block key for decrypting the block data is generated from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data.

37. The method according to claim 35, wherein in the decrypting step, a title-unique key is generated from a master key stored in the information player, disc ID

being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and the block key is generated from the title-unique key and block seed.

38. The method according to claim 35, wherein in the decrypting step, only data included in the block data and excluding data in a leading area including a block seed of the block data is decrypted with the block key in the encryption of the block data.

39. The method according to claim 35, wherein in the decrypting step, a title-unique key is generated from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated is taken as a key for an encryption function, the block seed is placed into the encryption function, and a result of the placement is outputted as a block key.

40. The method according to claim 35, wherein in the decrypting step, a title-unique key is generated from a master key stored in the information player, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, the title-unique key thus generated and block seed are placed into a one-way function, and a result of the placement is outputted as a block key.

41. The method according to claim 35, wherein in the decrypting step, a device-unique key is generated from any of an LSI key stored in an LSI included in the cryptography means, device key stored in the information player, medium key stored

in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and a block key for decrypting the block data is generated from the device-unique key thus generated and block seed.

42. The method according to claim 35, wherein in the decrypting step, the block data decryption with the block key is made according to a DES algorithm.

43. The method according to claim 35, further comprising the step of identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not playback from the recording medium is allowed.

44. The method according to claim 35, further comprising the step of identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not playback from the recording medium is allowed.

45. A recording medium having recorded therein a block data including more than one packet included in a transport stream and having an arrival time stamp (ATS) appended to each of the packets, the block data including:

an unencrypted data part having a block seed including the arrival time stamp (ATS) from which there is generated a block key for encrypting the block data; and

an encrypted data part having been encrypted with the block key.

46. A program serving medium which serves a computer program under which recording of information to a recording medium is done in a computer system, the

computer program comprising the steps of:

appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream; and

generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated.

47. A program serving medium which serves a computer program under which playback of information from a recording medium is done in a computer system, the computer program comprising the steps of:

generating a block key for decrypting encrypted data in a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and

processing a transport stream to control data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted in the cryptographic step.